Anno 2 - N. 33
11 Settembre - 25 Settembre 2003

Boss: theguilty@hackerjournal.it

Editor: grand@hackerjournal.it

Contributors: Bismark.it, Fabio Benedetti, Guglielmo Cancelli, Gaia, Nicola D'Agostino, Lele, Roberto "decOder" Enea, >>>----Robin---->, Lidia

DTP: Cesare Salgaro

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Copertina: Zocdesign.com

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, viale Forlanini, 23
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hãk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

BUON SENSO CERCASI

La lotta alle normative sui brevetti software ha dato un primo risultato: la votazione sulla nuova normativa Europea, che avrebbe effetti devastanti sulla libertà di sviluppare software, è stata rimandata di una ventina di giorni, e si terrà il 22 settembre nel corso di una riunione plenaria del Parlamento Europeo. Il motivo del rinvio è legato alle proteste che si sono tenute a fine agosto a Bruxelles, e alle lettere aperte di ricercatori, scienziati ed economisti che hanno duramente criticato la proposta di legge in discussione. I legislatori comunitari hanno voluto prendersi un po' di tempo per valutare meglio la situazione, e soprattutto le conseguenze del provvedimento. E, probabilmente, vogliono allargare il numero dei votanti, per distribuire quella che ormai percepiscono come una responsabilità molto grande.

Già, perché se passasse la legge così come è stata proposta, le conseguenze sarebbero devastanti. Anche se si tratta di argomenti già trattati su questa rivista, vale la pena di precisare alcune cosucce. La proposta è così restrittiva che, oltre a vietare di copiare intere porzioni di codice, si estende anche a idee, paradigmi e singoli algoritmi così banali che qualsiasi studente delle superiori potrebbe ritrovarsi a violare il copyright di qualche azienda solo facendo i compiti. Peggio: gran parte del suo programma di studi potrebbe essere cancellato perché è proprietà di questa o di quella azienda.

Alcuni esempi? In questi giorni, visitando l'home page dell'Associazione Software Libero (www.softwarelibero.it) si viene accolti dalla scritta "Attendere prego", accompagnata dalla classica barra di avanzamento. Subito dopo, una scritta ci avvisa che è in corso una violazione di copyright: la barra di scorrimento è brevettata, così come 30.000 altri brevetti europei sul software che rischiano di avere corso legale. E quello della barra di scorrimento non è che un esempio: gli esempi spaziano dai meccanismi per decodificare il movimento del mouse all'uso dell'operatore XOR per visualizzare la finestra in primo piano nei sistemi operativi grafici. La cosa scandalosa è che molto spesso le aziende che detengono i diritti di sfruttamento di queste "invenzioni", non hanno nulla a che fare con gli effettivi inventori: basta individuare un'idea che ha una parvenza di originalità, far scrivere una bella descrizione da un avvocato specialista in questo campo, e arrivare per primi alla fila dell'Ufficio Brevetti. Ufficio che non si preoccuperà di valutare se l'idea che si sta cercando di brevettare è valida e unica, o se si tratta della "scoperta dell'acqua calda", semplicemente perché non è tenuto a verificare né appurare nulla. E così potrebbe succedere anche da noi quel che è capitato in Australia, dove per sensibilizzare l'opinione pubblica su questo tema, uno sviluppatore è riuscito a ottenere il brevetto per... la ruota! Riuscite a immaginare a che punto sarebbe l'evoluzione umana se davvero l'invenzione della ruota fosse appannaggio esclusivo di una sola azienda? La stessa cosa sta per avvenire nel campo del software, se non ci sbrighiamo tutti a fare qualcosa. Le informazioni e le istruzioni su come mobilitarsi le trovate nel già citato sito dell'Associazione Software Libero.

grand@hackerjournal.it

Saremo di nuovo in edicola Giovedì 25 settembre !

E c'è pure L'HACK BLOG

Il prolifico Bismark, nel mese di Agosto ha aggiunto un nuovo servizio per gli utenti registrati del sito di HJ: un blog personale che puoi usare per pubblicare il tuo diario, o un sito con appunti di qualsiasi genere. Per chi non lo sapesse, un blog è un minisito Web creato da un sistema di pubblicazione automatica, che permette di mettere subito online i propri contenuti senza bisogno di scrivere una sola riga di codice html, e gli articoli pubblicati possono anche essere commentati dai visitatori. Per questo, è l'ideale per siti da aggiornare frequentemente, come i diari appunto, o siti di una comunità o gruppo di amici, che possono rimanere sempre informati sulle ultime novità.

Se anche tu vuoi far parte della blog-revolution, corri subito ad aprire il tuo blog su hackerjournal.it

FREE HACK NET

Per chi in Agosto si fosse perso l'annuncio, lo ripetiamo.
Dal mese di luglio è attivo il servizio di collegamento a Internet targato Hacker Journal: indirizzo email @hackerjournal.it con 5 Mbyte, accesso super veloce fino a 128 Kbit al secondo (ISDN multilink PPP), server newsgroup, controllo anti virus e anti spam. Corri subito a iscriverti all'indirizzo www.hackerjournal.it/freeinternet

TRY2HACK RELOADED

La classifica dei campioni

Classifica

Campioni HackGame

N.	Nick	Iscritto il	Totale giorni
1	Pablo	18 giu 03	3
2	ISetol	19 giu 03	3
3	dos622	17 giu 03	5
4	K4u5	17 lug 03	20
5	NeoVR	8 lug 03	24
6	winsteel	13 lug 03	24
7	at4rgate	16 lug 03	33
8	TheLord	29 lug 03	35
9	Gusto Delposto	30 giu 03	38
10	xmanoid	27 giu 03	43

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: ness1
pass: scappell8

mailto:
redazione@hackerjournal.it

HJ FOR EVER

Ciao ragazzi non è stato copiato all'originale per ovvi motivi di tutela del marchio registrato, ma che ne dite? "Ma avrò dei problemi in spiaggia con questo tatuaggio?" Spero di rivedere anche quest'anno lo stand di H.J in Fiera a Milano più grande e più bello di tutti gli altri.

Massimo da Monza

Ti confesso che vedere che qualcuno si fa un tatuaggio ispirato a ciò che fai, la cosa fa venire i brividi. Da un lato, c'è l'orgoglio e la soddisfazione di rappresentare qualcosa di importante per i lettori; dall'altro, la paura di essere presi (e di prendersi) un po' troppo sul serio. Di smettere di essere persone, idee e intenzioni per diventare simboli. Come diceva anni fa Giovanni Lindo Ferretti in un disco dei CSI: "Non fare di me un idolo mi brucerò, se divento un megafono m'incepperò, cosa fare non fare non lo so, quando dove perché riguarda solo me". Passando a Smau, stai tranquillo: non mancheremo neanche quest'anno. Saremo al Padiglione 15/II, stand A26.

SCUOLA, LIBRI E HACKER

mi poptresti consigliare un libro che insegni a usare linux in modo semplice?(il mio preferito è Madrake 8.0, mi sta simpatico!:-))Poi vorrei un parere...quest'anno sto per incomiciare le superiori(dovrei essere in 4ta)...come perito informatico...Questa scuola mi sara utile per diventare un hacker un po seria?!:-/Aspetto tua risposta...(molto attesa)

Alitaprincess

Libri e scuola possono aiutare a diventare Hacker, ma non sono né una condizione sufficiente, né necessaria. Impara a farti domande; cerca di capire come funziona un programma, un computer, un tostapane. E quando lo hai capito, passa a qualcosa di nuovo e più stimolante, usando tutto ciò che hai a disposizione per imparare cose nuove, dai professori ai libri che puoi trovare in ogni libreria ben fornita. In bocca al lupo.

SCOVARE I DIALER

Nel numero 30 di HJ, a pag. 4 appare un riquadro con il titolo "TRUCCHI ANTI DIALER" a firma di badboy84, in cui manca un dato essenziale. Per poter vedere la cartella "dati applicazioni" bisogna visualizzarla e, quindi, andare su PANNELLO DI CONTROLLO/OPZIONI CARTELLA/VISUALIZZAZIONE. Alla voce "cartelle e file nascosti" attivare "visualizza cartelle e file nascosti". Dopodichè si può iniziare la procedura. Comunque, il file RASPHONE.PBK è raggiungibile in maniera più semplice, seguendo il percorso C:/WINDOWS/SYSTEM32/RASPHONE.PBK. Concludo specificando che in tale file sono contenute tutte le connessioni e con copia/incolla lo potete trasferire dove meglio vi aggrada.

Blue Chip

Grazie per la precisazione.

Tech Humor

Un display LCD dovrebbe servire per risparmiare spazio sulla scrivania; questo "modder" invece lo ha montato nell'involucro di un monitor tradizionale, ma ci ha messo dentro anche tutti i componenti del computer, montando i lettori e le interfacce sulla cornice del monitor stesso.
Ce n'è di gente con del tempo da perdere, eh?

Fabio M.

MANNAGGIA AL CALDO

Ciao RedaZ, spero che farete una correzione sul trafiletto "A volte ritornano", pubblicato a pagina 6 del n. 31. Altrimenti tutti i nostri tentativi per spingere gli utenti a capire la vera etica Hacker, vanno a farsi friggere...

Neuromante

La notizia di cui parla Neuromante termina con una frase infelice: "Si sa, ogni porta per un hacker è un invito a entrare". Il termine hacker è evidentemente usato a sproposito: andava corretto in "cracker", o sinonimi. Di tanto in tanto, anche alcuni nostri collaboratori confondono i termini, e in genere la redazione ci mette una toppa. Questa volta invece, complice il caldo e le vacanze estive, l'errore è passato in stampa (insieme a qualche altro, in effetti).

RIAVVII IMPROVVISI

Da un po' di tempo a questa parte, di tanto in tanto mi compare un avviso che dice che il mio computer verrà riavviato in 60 secondi, cosa che puntualmente avviene. Devo forse cambiare qualche impostazione? Magari ho fatto qualcosa di sbagliato (ogni tanto provo qualche programma nuovo, e a volte combino qualche casino...).

Silente

Tra i tanti programmi che provi, ti consiglio di installare un firewall. Probabilmente i sei beccato il virus Blaster (MSBLAST), che oltre allo spiacevole effetto collaterale che descrivi, è programmato per attaccare periodicamente il sito Windows Update di Microsoft. Il virus una volta tanto non si diffonde per posta elettronica, ma direttamente attaccando le macchine collegate in rete. L'attacco non è efficace se sulla macchina è installato un firewall (anche il gratuito ZoneAlarm va benissimo). Siccome sei già infetto, oltre a installare il firewall, dovresti anche rimuovere il virus. Trovi le istruzioni sul sito http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A

SFOGO DI UN "VECCHIO" HACKER

Carissimi amici di H.J., innanzitutto i miei più vivi complimenti per una rivista libera da legacci publicitari e di qualità, chi vi scrive è un vecchio hacker nel senso più puro della parola, son anni che faccio l'hacker, ossia smonto tutto ciò di cui voglio capirne il funzionamento, ho iniziato a 7 anni smontando motorini elettrici e lavatrici per usarne i pezzi per altre applicazioni o per migliorarne il funzionamento, sterei ed apparecchiature eletriche e meccaniche, ho fatto volare il mio motorino garelli a 100 all'ora con un cacciavite una lima e qualche chiave fissa ed un imbuto, ho telefonato gratis per anni nelle vekkie kabine a gettoni, ho fatto benzina gratis ai distributori self service a cassetto e no, ho viaggiato con biglietti a modo loro crakkati per l'autobus, sempre studiando il funzionamento dei vari meccanismi, infine ho usato vari computers durante la mia vita, Amiga, Vic 20, Vic 64, 128, 386, 486, pentium vari, vari sistemi operativi, dai basilari ai Mac, Windows, Linux ma non ho mai avuto il tempo per poter studiare i vari linguaggi macchina, son rimasto un hacker troglodita, ma pur sempre un vostro avo, e come tale, quando leggo lettere a voi indirizzate, mi rammarico per certi ragionamenti fatti da hacker moderni, tutta questa vanteria sulle proprie supposte capacità mi spiazzano non poco, io l'hacker lo facevo per sola mia soddisfazione non per vanteria o per esser osannato da chichessia, mentre ora leggo solo di gente che cerca fama e gloria, passando sulla testa di altra gente e causando loro danni solo per dimostrare al mondo quanto siano bravi ed intelligenti, attacando siti web di gente che per semplice dimenticanza od ignoranza con conoscono quella falla o la tal patch.Cosa voglio dire con ciò, non dimenticate mai l'umiltà e tralasciate l'arroganza, è l'uomo umile che crea grandi cose, lo sbruffone è destinato solo alle più pessime figuracce, perchè sulla sua strada troverà sempre uno più sbruffone di lui.Perseverate nel vostro lavoro di hackeraggio, migliorate i sistemi ed i software affinchè domani l'uomo possa vivere più comodo, per un mondo migliore, lasciate stare tutto ciò che è distruttivo solo per pura vanagloria, io vi ammiro e vi stimo, ma siate costruttivi.Riguardo i software proprietari, non siate così drastici nei giudizi, per ogni s.p. in rete ne trovate almeno 10 altrettanto validi e gratis, lo sò che le software house ci speculano ma la nostra miglior arma è non comprarli se son troppo costosi, non sputargli contro.Infine per quanto riguarda la nusica in rete, tutte quelle polemiche, la gente registra la musica da secoli ormai in modo gratuito, che c'è di tanto strano? Pensate forse che 30 anni fà non si poteva collegare il tv allo stereo e registrare S.Remo su una qualsiasi cassetta stereo7? Non è cambiato nulla in sostanza, la gente lo fà solo per risparmiare qualche soldino, tranne comprare poi il disco completo dell'artista preferito, perchè gli artisti validi son pochi, e quelli vendono lo stesso nonostante l'MP3.Solo una cosa è cambiata, il prezzo dei dischi, ora è esorbitante! Con questo mio sfogo, vi saluto, io non son programmatore, nè ormai hacker perchè ho un lavoro ed una famiglia da mandare avanti, non ne ho il tempo, perciò porgo a voi nuove generazioni i miei più sentiti omaggi ed auguri per un proficuo lavoro nell'informatica. Non siate stupidi, perché come disse Forest Gump - Stupido è chi stupido fà!!- Ciao a tutti e buon lavoro!!

NEWS

NUMERI

VIDEOGIOCHI: QUALCHE NUMERO

(Secondo un sondaggio pubblicato da Peter D.Hart Research per conto dalla Entertainment Software Association)

DONNE CONTRO UOMINI: 1-0

Il 26% dei giocatori sono donne di 18 o più anni, contro il 21% di maschi tra i 6 e i 17

MA GLI UOMINI VINCONO ANCORA

Il 38% dei giocatori sono uomini dai 18 anni in su, mentre le ragazze da 6 a 17 anni non superano il 12% del totale

VIVERE GIOCANDO

Il giocatore medio trascorre circa 6,5 ore alla settimana giocando, contro le 7,3 ore dei ragazzi tra i 6 e i 17 anni

GIOCATORI PIÙ MATURI

Sul totale di giochi venduti nel 2002, il 13,2% riportava l'etichetta "M" (mature) contro il 9,9% del 2001 e l'8% del 2000

GIOCATORI ULTRACINQUANTENNI

il 17% della popolazione dei giocatori di videogame è costituita da ultracinquantenni, contro il 13% di tre anni fa

BUONGIORNO VITAMINIC SBARCA IN KUWAIT

Buongiorno Vitaminic, che si occupa di Servizi Mobili Interattivi, e Wataniya Telecom, principale operatore di telecomunicazioni in Medio Oriente, hanno annunciato il lancio di nuovi servizi forniti da Buongiorno Vitaminic per il mercato delle comunicazioni mobili in Kuwait. I servizi offerti includono suonerie, loghi, servizi SMS informativi e contenuti multimediali innovativi, come gli MMS. Saranno offerti agli oltre 770.000 clienti di Wataniya Telecom nel pacchetto di servizi Action - gamma di servizi GPRS e MMS dell'operatore che si posiziona come la più ampia disponibile nel Medio Oriente - e tramite Internet nella sezione Funtec del sito web aziendale, all'interno di specifiche B! zone (www.wataniya.com/funtec).

L'ASSOCIAZIONE SOFTWARE LIBERO CONTRO I BREVETTI

L'Associazione Software Libero protesta contro l'Unione Europea. Pietra dello scandalo: il Parlamento Europeo, sollecitato dalla BSA, valuterà la proposta sulla brevettabilità delle innovazioni software. Secondo l'Associazione Software Libero, è già stato dimostrato negli Stati Uniti che il sistema brevettuale, esteso al software da 20 anni, ha rallentato l'innovazione invece che incoraggiarla, spostando i fondi destinati originariamente a ricerca e sviluppo verso i dipartimenti legali delle grosse multinazionali che si occupano a tempo pieno di costose cause brevettuali. Un tale sistema imporrebbe degli oneri eccessivi per le piccole e medie imprese europee, vero motore dello sviluppo software continentale, e le renderebbe succubi di quelle poche grosse aziende, in maggioranza extraeuropee, che posseggono grandi portafogli di brevetti software.

UNO SMARTPHONE CHE FUNZIONA CON LINUX

Si chiama A760 ed è uno smartphone che funziona con il sistema operativo Linux. Motorola l'ha presentato a Taiwan, insieme ad altri otto cellulari in arrivo nei prossimi mesi, in occasione dell'International Telecommunications & Networking Show. L'A760 unisce un dispositivo informatico, un riproduttore video, un player musicale e uno strumento per l'instant messaging. Inizialmente sarà disponibile soltanto in Asia, ma le uscite in Europa e in America sono previste a breve. Motorola ha dichiarato di voler impiegare Linux per la maggior parte dei suoi futuri cellulari, inclusi quelli più economici.

AMIGHI DI TUTTO IL MONDO...

Torna anche quest'anno, nella sua settima edizione, Pianeta Amiga, lo storico appuntamento dedicato a tutti i fan di Amiga e delle piattaforme alternative. Come ormai è tradizione l'evento si svolgera sabato 20 e domenica 21 settembre presso il Pala Esposizioni di Empoli (FI).
L'organizzazione, a cura di Jasa Communication con l'apporto di varie realtà del mondo Amiga e delle piattaforme alternative, preannuncia un'edizione ricchissima di novità tra le quali, la più importante, che sicuramente non potrà che entusiasmare tutti coloro che ne hanno apprezzato l'ineguagliabile potenza ed innovatività, è il ritorno, con nuovi modelli destinati al mercato consumer e professionale, di Amiga con l'attesissimo Amiga One accompagnato dall'ultima revisione del suo pionieristico sistema operativo Amiga OS 4.0.

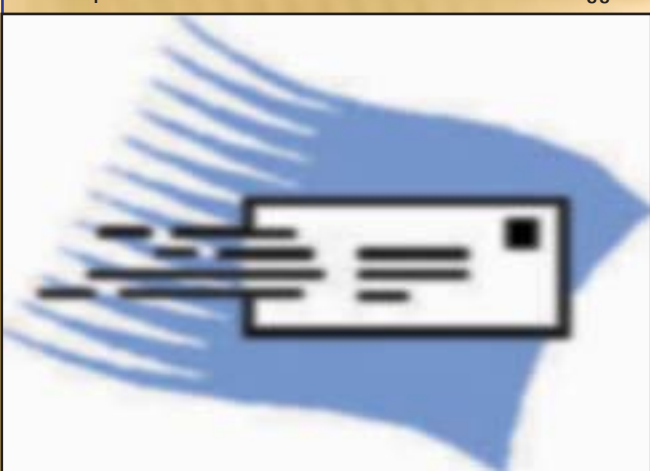
UN EVENTO DEDICATO AL MONDO MAC

Domenica 21 Settembre si terrà a Milano, presso il Mac@Work (Via Carducci, angolo galleria Borella, MM S.Ambrogio o Cadorna), il MacWave, il primo ritrovo off-line di ilMac.net, la rivista on-line per utenti Mac, al quale sono invitati tutti gli appassionati Mac-User d'Italia. Il programma per la giornata è molto ricco, ci sarà spazio per brevi sessioni dimostrative orientate all'open source, alla Rete e molto altro. Inoltre, sarà l'occasione per vedere dal vivo i nuovi PowerMac G5 e ammirare le nuove funzionalità di Panther, la nuova versione di Mac OS X. La partecipazione a quest'evento è gratuita e aperta a tutti. Per ulteriori informazioni e iscrizioni: www.ilmac.net/ilmacwave/

MULTIPLAYER CON DISPOSITIVI MOBILI

Si chiama N-Gage Arena il servizio di Nokia che permetterà ai patiti del multiplayer di giocare online anche con le console mobili. Disponibile a livello mondiale, l'N-Gage Arena sarà il punto d'incontro dell'intera comunità dei giocatori di tutto il mondo, che potranno sfidarsi su Internet. Il servizio sarà attivo a partire dal 7 ottobre 2003. I contenuti verranno inizialmente offerti in forma gratuita per un periodo di prova, per consentire ai giocatori di sperimentare il servizio. Il traffico dati sarà invece soggetto alle tariffe applicate dai diversi operatori telefonici.

E-MAIL: SEI GRADI DI SEPARAZIONE

Ci vogliono dalle cinque alle sette e-mail per raggiungere una persona sconosciuta dall'altra parte del mondo tramite il "passaparola" della posta elettronica. E' quanto è risultato da un esperimento condotto dal professor Duncan Watts, della Cornell University di New York, negli Stati Uniti. 61.168 persone di 166 differenti Paesi hanno preso parte alla ricerca. A ognuno di essi venivano forniti i dati di 18 persone da raggiungere con una e-mail, che però non poteva essere inviata direttamente ai soggetti interessati: il messaggio doveva essere inviato a un conoscente considerato potenzialmente "più vicino" al destinatario finale del messaggio. I soggetti da contattare erano stati scelti casualmente, e andavano da un professore americano a un poliziotto australiano, da un veterinario norvegese a una telefonista russa. I risultati della ricerca hanno indicato che nella maggioranza dei casi, per raggiungere la persona interessata sono state necessarie da cinque a sette e-mail. I ricercatori hanno tracciato 24.163 catene di messaggi. Di questi, solo 384 sono riusciti a raggiungere il destinatario finale.

SITI WEB

UN FINTO SITO AMICO

www.nosms.com/index_italia.php

Il benvenuto di questo sito parla da solo: "Benvenuto nella lista ufficiale di protezione SMS del sindacato internazionale Global Spam Protect Limited (GSP), per la protezione contro messaggi SMS indesiderati sui telefonini. Noi vi offriamo la possibilità di inserire il numero di telefono nel nostro sito e di proteggerlo contro gli SMS indesiderati di pubblicità (SPAM). Questo servizio è gratis e anonimo. Noi permettiamo alle compagnie che devono fare pubblicità di verificare le nostre liste, così possono eliminare i numeri di persone che non vogliono ricevere SMS." E' un sito che promette di "proteggere" il tuo numero di cellulare … ovviamente se inserisci il numero di cellulare ti becchi dodicimila messaggini stronzi. Occhio a non cascarci!!!

REGISTI IN ERBA

www.fanfilms.com

Il vostro sogno nel cassetto è diventare registi? Allora non potete perdervi questo sito con i filmati di registi in erba che ricostruiscono film famosi. E chissà…potreste mettere on-line anche il vostro!!!

VAFFANGOOGLE

www.vaffangoogle.tk

Una Home Page originale per il motore di ricerca più famoso del mondo.

DEFCON: UNA FESTA HACKER

Giunta all'undicesima edizione, la manifestazione Defcon è maturata, e ha trovato in quelle che erano gli eventi a contorno il vero spirito della manifestazione. Oltre ai seminari, le oltre tremila persone intervenute cercavano quell'atmosfera speciale che la comunità hacker è in grado di creare. Atmosfera che, ovviamente, noi non potevamo fare a meno di andare a respirare.

Las Vegas, Alexis Park, un piccolo hotel con tre piscine e qualche centinaio di stanze, un paio di isolati fuori dalle luci della Strip, stranamente senza le altrimenti onnipresenti slot machine. Uno, due e tre agosto; l'anno scorso c'erano 46 gradi, quest'anno il cielo è un poco coperto, e 37 gradi sembrano un tepore primaverile.

Defcon è dormiente fino alle undici del mattino, poi pigramente inizia ad animarsi. **Tre sono i percorsi che si tengono contemporaneamente** nelle diverse sezioni dell'albergo, un filone diverso per ogni giorno. Il venerdì è dedicato a incontri con i protagonisti (apre **Phil Zimmerman**, mister PGP, di recente affrancato da NAI), **Privacy**, **Anonimità** e al **Net recognition**. Sabato i filoni trattano invece i **problemi con la legge**, **attacco** e integrazione tra **Web e database**.

Mr. PGP si è finalmente affrancato dal Marchio NAI "Una backdoor in PGP messa da NAI? Quelli non sapevano neanche dove mettere una Front Door in PGP". Da queste parole capite che Phil non doveva avere una grande stima nel team della NAI...

Domenica è una giornata in sordina; gli stravizi del sabato notte (grande ballo Black and White fino all'alba e party in tutte le piscine dell'albergo) e la prospettiva di guidare nella notte per oltre mille miglia, decimano i partecipanti, che possono seguire le conferenze su **Worm e virus**, **Difesa e Sicurezza Fisica**, ma tutti aspettano la cerimonia di chiusura con le premiazioni alle quattro del pomeriggio.

Molte manifestazioni concorrenti a Defcon. Di seguito una breve descrizione dei concorsi e i loro esiti.

Root-fu (ex Capture the flag)

Il root-fu è certamente la competizione più importante della manifestazione. Quest'anno i **Ghetto Hackers**, che hanno vinto tre edizioni di Capture the Flag prima di ritirarsi e passare all'organizzazione, **hanno veramente fatto le cose in grande**: "Ci è costato più di 20.000 dollari, per ora non rilasceremo il codice al pubblico" dice Caesar, l'organizzatore della gara. Il software di cui parla Caesar è un CD con installato un servizio di advertising multimediale completo, che i team hanno ricevuto il primo giorno della manifestazione. Si facevano punti **riuscendo a mandare in onda i propri annunci pubblicitari e servizi multimediali sui server altrui**. Il sistema andava studiato per trovare i punti deboli, bloccarli sul proprio sito e sfruttarli al tempo stesso per insidiare i siti altrui. La maggior parte dei team era composta da una decina di componenti, salvo Immunity Linux, una Software House che è arrivata seconda lo scorso anno e che con venti esperti divisi in tre team avrebbe dovuto dominare la competizione questo anno. Il loro progetto era di migrare il sistema di pubblicazione sulla loro piattaforma **Immune Linux** per dimostrare la reale robustezza. Questo doppio lavoro li ha però penalizzati ed hanno dovuto accontentarsi del secondo posto, con enorme scorno. Auguri per il prossimo anno! Questa volta i vincitori sono stati i componenti del team **Anomaly**.

Caesar, di Ghetto Hackers, il responsabile dell'organizzazione del Root-Fu.
I team selezionati si sono dati battaglia in un salone con due video proiettori per tre giorni. "L'anno prossimo faremo un confronto diverso, probabilmente 48 ore di fila senza interruzioni [neanche per andare al bagno, penso io...]"

Il tabellone del Root-Fu mostra moltissime informazioni. Oltre al punteggio le palle verdi indicano se si sta usufruendo dei servizi di un altro server (rosse, haimè, è il contrario), mentre i cerchi concentrici indicano il numero dei servizi attivi.

WarDrive

"WarDrive is not a crime", questo lo slogan della gara di quest'anno. In effetti WarDrive è una occasione eccezionale per raccogliere informazioni su come le aziende e la scarsa conoscenza delle tecnologie **mettano in pericolo i dati e la sicurezza delle famiglie e delle aziende**. Il WarDriving consiste esclusivamente nel raccogliere le informazioni sulla localizzazione dei punti di accesso WI-FI, raccogliendo i dati sulla posizione geografica (GPS) e se è attivo il Wep o meno ed il nome di accesso della rete. Eseguendo un WarDrive con cadenza periodica si ottengono **dati su migliaia di punti di accesso**, e si capisce se gli utenti hanno imparato o meno a configurare gli appartai e non semplicemente a tirarli fuori dalla scatola e attaccarli alla corrente. Certo, se le aziende consegnassero il Wep attivo di default sarebbe meglio, ma questo aumenterebbe le chiamate al supporto perché è vero, configurare una rete sicura non è proprio facile!
Quest'anno ho seguito un team in macchina durante la ricerca (tutto ciò a est di Paradise Road per le qualifiche, e tutto quello ad ovest il giorno dopo, per la finale) e ho imparato molte cose sull'arte del WarDriving. **"Mai tentare di accedere alle reti!"** dice Erich, l'autista della macchina che percorre lentamente le strade di Las Vegas; e **"Mai guardare il monitor mentre guidi, bisogna sempre prima parcheggiare"** aggiunge. "Perché fai il WarDrving?" chiedo. **"Perché è un modo per aiutare la gente ad essere più sicura"**,

"Wardrive is not a Crime" è lo slogan della manifestazione. Il crimine vero è quello della banca davanti cui siamo passati che non usava WEP per la sua rete wireless. Non ci avrei creduto se non lo avessi visto con i miei occhi...

Wi-fi Shootout, categoria 6. Antenne potenziate direzionali o omnidirezionali autocostruite. Che ci crediate o no, con con 98 dollari da Home Depot, ASLRulz ha costruito una antenna capace di collegarsi a 56.668 Km di distanza! Magari non avrà l'omologazione, ma è difficile credere che a anche a questa distanza qualcuno possa ascoltare la vostra rete...

dice Erich, e se lo dice lui io gli credo. È divertente vedere intorno a noi le macchine rallentare e guardare con diffidenza la nostra macchina piena di antenne... **Il team di Erich trova circa 1200 punti di accesso il primo giorno**, si qualifica senza problemi alla finale e spera per la vittoria: ad ovest di Paradise, il giorno dopo. Ma questa è una comunità di Hacker, e il regolamento diceva “solo a ovest di Paradise”, senza specificare “quanto a ovest”. Un partecipante dell’altra squadra, quindi, è partito di notte e ha guidato verso Los Angeles, a ovest di Las Vegas e di Paradise. **Un Hack che la giuria ha premiato con la vittoria**, ma ha previsto di modificare il regolamento per l’anno prossimo, almeno includendo “all’interno dello stato del Nevada!”

Scavenger Hunt

La caccia al tesoro è un classico della manifestazione. Viene consegnata una lista di oggetti da trovare o di azioni da compiere (e documentare), ognuna con un valore in punti. La lista è lunga e bizzarra ed ha garantito agli organizzatori di ridersela a crepapelle alle spalle dei team. Cento punti valeva **la testa di una mucca** (nessun riferimento a ragazzi del “Cult of the dead Cow”, vero?), ma solo a condizione che venisse correttamente smaltita dal team dopo averla mostrata alla giuria, oppure **le foto dei partecipanti del team che pescavano nei laghi degli hotel-casinò Bellagio, Mirage e Venecian**. Altri ogetti erano semplicemente “imbarazzanti” da trovare, chiedere e mostrare, come **vibratori multifallo**, **presevativi** o **correre nudi per le sale...**
Ecco cosa hanno portato di interessante “The Winning Team”, arrivati secondi: cacciati dalla sicurezza in un Casinò, mangiata una banconota da 5 dollari, tiro a segno di una lattina di Guinness, un membro del team nella galera di Las Vegas (non provatelo a casa).

Cosa si vince alla caccia al tesoro? Ciarpame! Scatole e scatole di deliziosi reperti dal passato, incluso il giubbetto salvagente dell’American Airlines che il ragazzo al centro sfoggia.

La caccia al tesoro consiste nel rimediare oggetti e prove di aver compiuto alcune gesta in giro per Las Vegas. Certo alcune cose erano veramente difficili da trovare. Mangiare 20 bustine di dolcificante “Sweet and Low” (mio Dio, preferirei morire!), oppure iniziare una discussione animata davanti al vulcano del Mirage (sì, a Las Vegas c’è anche questo!), esprimendo dubbi sul fatto che il vulcano sia vero oppure no...

Hacker Jeopardy

Tra tutti gli eventi collegati a DefCon, questo, giunto alla decima edizione, è certamente il più antico. Con una formula tratta da un gioco televisivo americano (Jeopardy) i concorrenti sono tenuti a **dare le domande alle risposte che gli vengono proposte su diversi argomenti**, tutti correlati alla cultura tecnologica. Inoltre **si guadagnano punti consumando sostanze alcoliche**.
Molti record quest’anno: vinto il team che nelle eliminazioni ha avuto il più basso punteggio di sempre, con il più basso consumo di alcolici (4 bottiglie) ed è arrivato secondo un team che ha totalizzato il più alto consumo di birre con 23 bottiglie...)
Ma cosa aveva di particolare il team **Hackers & Hardware Whore** (letteramente Hacker e puttane dell’hardware) per fare parlare tanto di sé? Facile: **uno dei componenti era Kevin Mitnick...**
Durante la premiazione Kevin è stato accolto da un’ ovazione.

Un gioco a premi particolare con categorie e domande particolari: sapreste dare la soluzione a questa equazione?

Hackers & Hardware Whore vincono la finale della manifestazione. L’entusiasmo del team è visibile. E pensare che hanno bevuto solo 4 birre…

Lockpicking (aprire serrature)

Nonostante la scandalosa sensazione di illegalità che la gara di scassinamento può suscitare, essa nasconde in realtà una autentica e "sana" tradizione Hacker. Agli albori dell'hacking, al MIT si iniziò a proteggere gli accessi alle sale computer con delle serrature, quindi cosa c'era di sbagliato nell'imparare ad aprire le semplici serrature americane, per condividere con la comunità le preziose e inutilizzate risorse del college? Moltissimi iscritti, e divertimento per tutti. Nelle eliminatorie **il tempo migliore è stato di sei secondi**, ma l'autore è poi crollato nelle semifinali.

Una serratura elttronica per misurare i tempi con grande precisione. Alcuni dei partecipanti aprono un luchetto in sei secondi. Al MIT, ai tempi d'oro non dovevano avere vita facile a tenere chiuse le porte!

Con strumenti di precisione ed occhiali luminosi, questo ragazzo si impegna a fondo per scassinare le tre serrature che gli daranno accesso alle finali!

Wi-fi Shootout

Quanti chilometri si possono fare con un collegamento WI FI? Ecco le risposte:

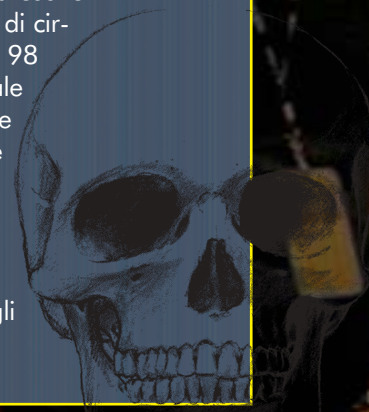
CAT 1: Stock/antenne commerciali omnidirezionli
Distanza: 16,3840 Km, **Team:** 4DI

CAT 2: Stock/antenne commerciali direzionali
Distanza: 16,3514 Km, **Team:** 4DI

CAT 4: Antenne direzionali autocostruite
Distanza: 8,2157 Km, **Team:** APP

CAT 5: Antenne potenziate direzionali o omnidirezionali commerciali
Distanza: 23,9662 Km, **Team:** 5G Wireless Communications, Inc.

CAT 6: Antenne potenziate direzionali o omnidirezionali autocostruite
Distanza: 56,668 Km, **Team:** ASLRulz

Il team ASLRulz ha costruito la sua antenna di circa 4 metri con 98 dollari di materiale preso da Home Depot, un grande magazzino di materiale per la costruzione e la casa, molto diffuso e fornito negli Stati Uniti.

Spot the fed!

Individuare gli agenti federali a Defcon è una abitudine inveterata. Il gioco è facile e tutti sono tenuti a partecipare. In qualsiasi momento si individui un federale, si ha il diritto di fermare la conferenza e tutti mettono ai voti se l'indiziato è un federale o no. Chi indovina vince la maglietta **"Ho beccato un federale"**, e il federale la maglietta **"Sono un Federale"**. Valgono solo i federali che non vogliono essere beccati! Non ho i dati di questo anno, ma in genere ne vengono trovati sette o otto ogni anno.

CannonBall

Sulla gara CannonBall, da Los Angeles a Las Vegas in macchina, stendiamo un velo pietoso vista l'**alta illegalità e pericolosità della competizione**: il vincitore ha viaggiato a oltre 130 miglia (quasi 200 Km all'ora) con un limite di 75. Se lo sceriffo lo avesse beccato lo avrebbe portato dal giudice e non se la sarebbe cavata con meno di 7 giorni di carcere e una multa gigantesca. Nessuno dei sette partecipanti è stato fermato dalla polizia...

Guglielmo Cancelli

Le nuove frontiere dell'Hacking

Sabato due agosto, all'alba delle undici del mattino, un italiano attira grande attenzione riempiendo la sala più grande della conferenza, la sala Apollo. Roberto Preatoni (aka SyS64738) è infatti l'ideatore di Zone-H, il sito che –tra i tanti servizi– tiene il conto degli episodi di attacco che si verificano sulla Rete. Si potrebbe dire che "non è successo se Zone-H non lo documenta".

Questa diapositiva, tratta dalla presentazione di DefCon, mostra quali siano i punti deboli e più probabilmente soggetti ad attacco, nella rete che collega il palmare ai contenuti.

Al centro delle polemiche per essere stato trascinato senza alcuna volontà (o consultazione preventiva) a fare da arbitro alla fallimentare gara sull'hackeraggio di 6000 siti in un giorno, Roberto presenta a DefCon gli ultimi ritrovati della tecnologia cellulare 3G, mostrando i limiti e i pericoli impliciti che la nuova tecnologia porterà.

La sua equazione è semplice: la card del telefono è un dispositivo intelligente che garantisce l'identificazione; Windows CE è un sistema intrinsecamente insicuro, perché non è nato per essere collegato in rete. I modelli di memoria e dati rendono intrinsecamente insicuro il dispositivo, visto che la memoria è condivisa in modo dinamico e quindi applicazioni che entrino in funzione successivamente trovano ancora i dati di quelle precedenti. La linea di trasmissione è cifrata, ma solo per la parte aerea: poi il traffico voce e dati viaggia in chiaro sulle linee dati del provider e poi su Internet.

Marcio fin dalle radici

In pratica il punto migliore dove compromettere il sistema è senza dubbio il palmare. Già Microsoft ha iniziato a commettere i primi errori marchiani, quando ha pubblicato SQL per CE con incluso un bellissimo server Http che pubblicava tutte le cartelle del palmare. A merito di MS va detto che ha immediatamente ritirato il prodotto, che era ancora in fase di beta, per correggere questo problema.

Il sistema Windows CE riutilizza la memoria senza pulirla. Diverse applicazioni possono facilmente accedere ai dati che l'applicazione precedente ha lasciato in memoria. Inoltre, c'è una certa pigrizia nell'aggiornare il sistema, come mostra la parte destra dell'immagine; un buco segnalato mesi e mesi fa!

È interessante notare come un'applicazione pirata possa facilmente accendere microfono o telecamera del cellulare per spiarci e, addirittura, quando saranno integrati i GPS, trovarci e seguirci con una precisione di quattro metri (i sistemi attuali di localizzazione attraverso le celle hanno un errore di un centinaio di metri).

Un frigorifero su Internet; riusciranno le nostre bistecche a sopravvivere al ping of death?

La soluzione è semplice. Dire no ai palmari di adesso super integrati, e tenere divisi telefono e palmare. Le industrie non documentano quanto grave e facile possa essere la compromissione della sicurezza, quasi inesistente al vero, e quindi gli utenti non vengono sensibilizzati ai reali pericoli che corrono. Piccoli, funzionali, addirittura sexy, rischiamo per la comodità di uso di portarci in tasca il nostro cavallo di troia, per poi mostrare sorpresa e rabbia quando scopriamo che qualcuno ha usato la nostra carta di credito.

Quali sono i punti di accesso?

I soliti, solo che sul palmare sono ancora meno protetti:

- Buchi del Sistema Operativo
- Le porte aperte
- Cavalli di Troia e Virus (per mail e programmi infetti scaricati)
- Componenti di serie difettosi (Media Player, Browser etc)
- Difetti del web server
- Attaccare i punti deboli delle applicazioni più diffuse.

Spesa a rischio

Tutto questo senza prendere in considerazione lo sviluppo futuro degli elettrodomestici, connessi a Internet. Immaginate questo frigorifero Internet prodotto da LG. Pensate che LG si sia riscritto un browser per leggere la posta sull'Lcd della porta? Ovviamente no. Questo frigorifero utilizza una versione modificata di Windows 98. Modificata perché supporta il touch screen, altrimenti è lo stesso W98 che abbiamo usato per anni. E cosa basta per scongelare da remoto le nostre bistecche? Facile: PING -L 65535 miofrigo.casamia.it, un semplice Ping of death!

Roberto Preatoni (aka SyS64738), fondatore di Zone H, si gode il sole estivo durante l'intervista dopo la sua conferenza, davanti alla piscina dell'Alezis Park.

Ovviamente questi sono gli estremi del problema, ma non crediate che siano molto diversi da quelli che ci riserva il futuro,0 più prossimo a venire di quanto non immaginiamo.

Per i più curiosi...

Nella sezione Contenuti Extra del nostro sito potete trovare molti link sui sistemi cellulari di ultima generazione. Se invece volete contattare SyS64738, lo trovate su www.zone-h.org.

UN RIFUGIO CHE AFFONDA

L'idea non era male: una server farm situata fuori dai confini di ogni stato, per evitare cause e censure. Peccato che...

Nel numero 10 di Hacker Journal i nostri lettori hanno fatto conoscenza con **una delle iniziative più interessanti e ambiziose riguardo la gestione "sicura" dei dati su Internet**: il progetto HavenCo. Situato su Sealand, una ex-piattaforma militare al largo delle coste britanniche, requisita e dichiarata come "principato" (www.sealandgov.com) dopo la seconda guerra mondiale. Negli ultimi anni, HavenCo si è presentato come un rivoluzionario servizio che offre hosting sicuro e **teoricamente al riparo dalla longa manus di governi, agenzie e soggetti malintenzionati**.

Nel corso delle ultime settimane, l'alone di romanticismo attorno ai rack di computer situati nei piloni di cemento di Sealand **si è improvvisamente diradato** e si parla di problemi tecnici, organizzativi e amministrativi, dell'**influsso infausto del post-11 settembre**, di un progressivo e totale **disimpegno dei soci fondatori** e a **manovre poco chiare dei "regnanti" di Sealand**.

Su HavenCo si addensano nubi fosche che pongono dubbi sull'iniziativa stessa. Per fare un po' di luce sulla vicenda abbiamo interpellato direttamente uno dei personaggi chiave, **Ryan Lackey** (www.venona.com/rdl/resume.html), ex-socio fondatore di HavenCo, che è attualmente al lavoro su un libro (http://havenco.venona.com/) che narrerà i tre anni di attività di HavenCo.

Hacker Journal: Presentati ai lettori Di hacker Journal. Qual'è il tuo background formativo e professionale?

Ryan Lackey: Prima di HavenCo ho lavorato nei Caraibi ed altrove, sviluppando soluzioni software e-cash (pagamento elettronico), crittografiche ed altri strumenti per la salvaguardia della libertà individuale. Prima ancora sono stato uno studente universitario al MIT, negli Stati Uniti.

HJ: Di chi è stata l'idea di HavenCo? Sono vere le voci che parlano di un romanzo alla base della sua ispirazione?

RL: L'idea di fondo di un "data haven" è in realtà molto vec-

chia -probabilmente risale agli anni '60 o ancora prima- e se ne è discusso a lungo negli anni '80 e '90: sia i fondatori di HavenCo (io e numerosi altri attivisti statunitensi nel campo della crittografia e della difesa della privacy), sia Neal Stephenson (autore di "Cryptonomicon", il libro a cui ti stai riferendo) erano a conoscenza di queste discussioni ma non esiste un punto di contatto diretto tra i due. (Molto prima di Cryptonomicon, di Covi Dati si parla anche nel libro "Isole nella Rete", di Bruce Sterling, ndr).

HJ: Qual'è stato il tuo ruolo in HavenCo e quali erano le altre persone coinvolte?

RL: Io sono stato uno dei fondatori, insieme a Sean e Jo Hastings. Tutti e tre eravamo nei Caraibi e volevamo creare un 'datahaven' (letteralmente un 'rifugio per i dati' ndr). Il primo a investire su di noi è stato Avi Freedman; oltre a lui abbiamo avuto altri consiglieri e sostenitori nella fasi iniziali, tra cui Joichi Ito e Sameer Parekh, entrambi piuttosto noti negli ambienti della privacy e della crittografia.
Abbiamo individuato come base il "Principato di Sealand" e abbiamo stretto accordi commerciali con il suo "principe", Michael Bates, e i suoi soci.

HJ: Quali tecnologie sono state impiegate? Quali sistemi operativi? C'è qualche soluzione o hack hard/soft di cui sei particolarmente orgoglioso?

RL: Ho personalmente sviluppato numerose soluzioni tecnologiche prima e dopo HavenCo, ma queste non sono state usate se non in minima parte dai nostri clienti. Le cose di cui sono principalmente orgoglioso sono i sistemi per il pagamento anonimo e i router, sistemi di sicurezza e strumenti vari, tutti affidabili e open-source.
HavenCo aveva un budget abbastanza limitato e perlopiù ha operato con attrezzature un po' superate o sottostimate: l'intera connettività di HavenCo è all'incirca la stessa di un utente casalingo o un ufficio con una adsl o una connessione via cavo.
Ci sono circa 5 rack per ospitare computer ma non sono pieni di hardware dei clienti. Attraverso dei network probe è possibile verificare come ci siano attualmente meno di 20 clienti a HavenCo, cifra che nella realtà si aggira tra i 5 e 10.

HJ: E' vero che hai passato lunghi periodi sulla piattaforma, solo o quasi?

RL: Sealand era perlopiù presidiata da due persone alla volta: per gran parte del 2001 e del 2002 io sono stato uno dei due. Gli altri erano personale britannico addetto alla sicurezza o ai generatori e agli approvigionamenti via mare.

HJ: Cosa non ha funzionato nell'impresa HavenCo e quali sono state le pecche maggiori, secondo te?

RL: Il problema principale è che il "Governo di Sealand" ha violato il contratto stipulato con HavenCo e ha in pratica sottratto il patrimonio di HavenCo senza conferire nessuna azione agli investitori al contrario di quanto pattuito. Qui non si tratta solo degli interessi degli investitori ma del fatto che non ci si può aspettare che le persone affidino dei server Internet alla mercé di individui che violano i contratti.
HavenCo inoltre ha dei costi fissi relativamente alti rispetto agli introiti: dai prezzi alla clientela sul sito si può verificare come HavenCo non generi introiti degni di nota né tantomeno sia in grado di far fronte al deprezzamento dell'attrezzatura.
Un altro grave problema di HavenCo è la mancanza di un sistema di pagamento per i clienti, il che riduce notevolmente la domanda. Inoltre la situazione legale di Sealand continua a tenere lontani i clienti: il "governo di Sealand" ha costretto HavenCo a rifiutare clienti appetibili che non violavano assolutamente le clausole d'uso (http://www.havenco.com/legal/aup.html), con il risultato di aver tarpato le ali al progetto, ridotto a fare da hosting ad un

ristretto numero di server di clienti che desiderano "pavoneggiarsi".

HJ: Quando e come hai abbandonato HavenCo e quale ti risulta essere lo status attuale? In mano a chi è HavenCo-Sealand ora?

RL: Ho lasciato HavenCo nel dicembre del 2002 dopo che il "governo di Sealand" decise di voler prendere il controllo della società. Era palese che non avrebbero mai permesso a HavenCo di fare affari e prosperare accettando clienti che rispettavano le clausole d'uso ma che erano loro poco graditi.
Michael Bates, nella sua veste di CEO, ha più volte rifiutato o è stato incapace di emettere azioni come concordato e io ero sempre più preoccupato per le possibili ripercussioni a livello legale e di reputazione nel caso fossi rimasto ancora coinvolto nella società. La separazione è stata di mutuo accordo ma Michael Bates ed altri rappresentati di Sealand/HavenCo hanno violato gli accordi dopo soli cinque giorni dalla firma.
Ritengo che attualmente HavenCo sia in una situazione di "pilota automatico", con uno o due addetti alla sicurezza sul luogo e Bates alle redini della ditta.

HJ: Cosa pensi di fare adesso? Ritieni ancora l'idea alla base di HavenCo valida? Cosa è 'Metacolo'?

RL: Penso che l'idea di un 'datahaven' sia fondamentalmente buona ma che il modello HavenCo abbia alcune gravi pecche:

- Creare una sede unica e centralizzata sotto il controllo di un gruppo di persone rappresenta un potenziale rischio, sia dal punto di vista legale, sia quello tecnico.
- Dal punto di vista tecnico, i clienti necessitano di replicazione e maggiore affidabilità e capacità della connessione.
- L'unico modo di garantire la sicurezza è tramite hardware resistente alla manipolazione/effrazione e grazie all'uso della crittografia: le regole aziendali possono essere infrante da impiegati disonesti o da attacchi esterni (tribunali, governi, criminali, ecc.).
- Un'organizzazione come HavenCo ridotta numericamente e dedita alla segretezza ma che non diffonde pubblicamente i dettagli tecnici non dovrebbe godere di fiducia. Ci si dovrebbe fidare solo delle ditte che forniscono informazioni complete e permettono un'analisi approfondita dei prodotti offerti.
- Senza un'offerta integrata di servizi (pagamento, sviluppo, implementazione, hosting, ecc.) per i clienti è praticamente impossibile affidarsi ad un server 'off-shore', ergo: c'è poca domanda.
Questi sono i princìpi che hanno ispirato la mia nuova società, Metacolo (www.metacolo.com/): fornirà anonimità sotto forma di hardware, software e servizi a chi ne ha bisogno, ma affidandosi alla "replicazione" dei server, di sistemi resistenti all'effrazione e le cui specifiche crittografiche sono pubblicamente diffuse e 'aperte'. Metacolo ha datacenter in numerose località sparse in giro per il mondo e utenti in numerosi settori. E' nei nostri piani offrire un ampio ventaglio di servizi, quali pagamenti anonimi, per cui c'è una richiesta concreta, richiesta che siamo decisi a voler e poter soddisfare.

Nicola D'Agostino
dagostino@nezmar.com

Ringraziamo Ryan Lackey per le immagini.
Thanks to Ryan Lackey for providing pictures.

QUALCHE DATO SULLA CONNETTIVITÀ DI HAVENCO/SEALAND

Il motto di HavenCo, riportato anche sul sito web, è "the free world just milliseconds away": il mondo libero a millisecondi di distanza. Secondo i piani originari la connettività di HavenCo, per garantire maggiore affidabilità, doveva essere ridondante e fornita da tre provider e in tre modalità diverse: una connessione via microonde, una via cavi subacquei e una via satellite.
Pochi sanno che per i primi tempi, fino all'inverno del 2000 per l'esattezza, solo una di queste fu attivata e che i server di HavenCo si appoggiavano a dei miseri 128k via satellite.
Oggigiorno i server di HavenCo sono online e raggiungibili al range di IP da 217.64.32.0 a 217.64.32.20 e, secondo una relazione presentata da Lackey al recente Defcon 11 a Las Vegas, in teoria sarebbero sufficienti 2Mbps di traffico per un attacco Denial Of Service per rendere inaccessibile il network e quindi bloccare in toto le attività di HavenCo.

24_27_hj33_ar 3-09-2003 9:40 Pagina 24

DATI IN ORDINE CON GLI ARRAY

Proseguiamo nella nostra panoramica sui principi base della programmazione, validi per ogni linguaggio che si vuole imparare.

Molto spesso, per i motivi più disparati, si ha la necessità di maneggiare e archiviare **una serie di dati omogenei fra loro**; ad esempio una lista di nomi, di numeri telefonici, una sequenza di numeri e così via. Sarebbe alquanto scomodo dichiarare (creare e nominare) tante variabili quanti sono i dati che vogliamo trattare.
Quello che fa al caso nostro, per memorizzare e gestire questi dati, è una particolare struttura che in informatica prende il nome di **array** (in italiano è comunemente usato anche il termine vettore, ma più spesso si usa la dizione inglese).

>> Che cosa è un array?

Un'ottima rappresentazione per un array è immaginarlo come **uno schedario in cui vi sono una serie di cassetti**, all'interno dei quali sono archiviati (memorizzati) dei documenti.
Se volessimo accedere ad un documento (un semplice dato nel nostro caso) contenuto all'interno dello schedario, dobbiamo prima individuare lo schedario (**nome dell'array**) e quindi il numero del cassetto (**indice dell'array**) e infine potremmo leggere o memorizzare il dato.
Nella fase dichiarativa (vedi articolo sul n. 32 di HJ) abbiamo visto come sia importante **riservare una porzione della memoria del computer per la gestione delle variabili**; in questo caso dovremo riservare memoria per il nostro array (schedario). Dovremo in tale fase **affibbiare un nome all'array**, determinarne la **dimensione** (ossia quanti elementi al massimo può contenere) e la **tipologia di dati che deve essere contenuta** all'interno del singolo cassetto (numeri interi, caratteri...).
Possiamo schematizzare questa fase (in un linguaggio formale) nella seguente maniera:

```
Nome_array
[Numero_totale_elementi]
Tipologia_dati_inseribili
```

Nel momento in cui voglio leggere o assegnare un valore ad una determinata casella (o cassetto) dell'array, non faremo altro che identificarlo in maniera univoca attraverso una chiamata del tipo:

```
Nome_array [Numero cassetto]
```

Attraverso una tale chiamata, il computer ha le coordinate per andare a individuare il dato che a questo punto può essere richiamato o sovrascritto a seconda delle esigenze.

>> Alcuni esempi

Vediamo come vengono usati solitamente gli array nei principali linguaggi di programmazione. La dichiarazione in linguaggio C di un array è la seguente:

```
int Pagine[16]
```

Abbiamo dichiarato un array di nome "Pagine" che può contenere al massimo 16 elementi e che tali elementi debbono essere degli interi; l'indice per il primo elemento è "0", mentre per l'ultimo elemento è "15" (quasi sempre, in informatica, si conta a partire da zero, e non da uno).
Qualora volessimo anche inizializzare l'array, ponendo un valore nullo in tutti gli elementi dell'array, l'istruzione da impartire sarebbe la seguente:

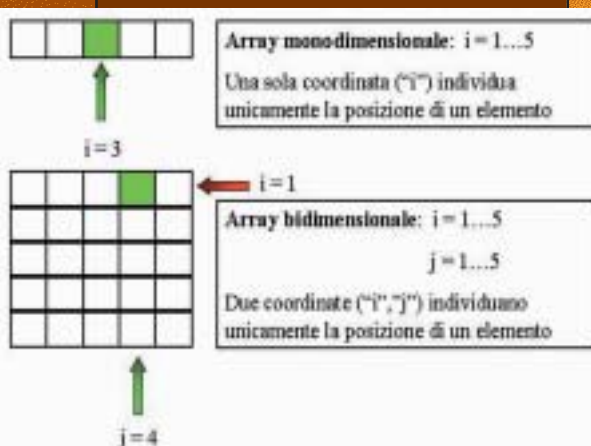
```
int Pagine[16] = {0};
```

Per quanto riguarda il C, nell'articolo precedente avevamo detto che in tale linguaggio non esiste il tipo variabile stringa; si ricorre perciò in questo caso alla definizione di un array di caratteri nella seguente maniera:

```
char Nome[ ] = "Robin";
```

Si è così dichiarato un array di caratteri (simulando quello che poi è effettivamente una stringa) di dimensione non precisata il cui contenuto è stato inizializzato a "Robin".
Vediamo, sempre a titolo di esempio, la dichiarazione in Pascal di un array bidimensionale.
Agli array bidimensionali viene generalmente assegnato il nome di "matrici" (sempre ricollegandoci alla matematica!).

```
var Forza4: array [1..6,
1..7] of integer
```

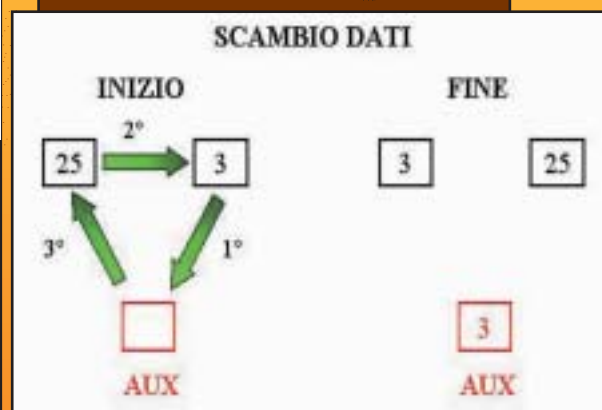
Abbiamo dichiarato un array bidimensionale (una matrice) di nome "Forza4" costituita da 6 righe e 7 colonne i cui elementi possono essere solamente degli interi.

>> Ordinare i dati

Molto spesso, in fase di inserimento, i dati saranno memorizzati all'interno dell'array **in maniera sequenziale, ma non ordinata**. Quello che vogliamo vedere è come poter **ordinare i vari elementi dell'array**. Per rendere l'idea faremo riferimento alla seguente sequenza di dati che vogliamo ri-memorizzare in maniera ordinata; per semplicità ipotizzeremo che il nostro array sia composto da 5 elementi e che la tipologia di dati trattata sia caratterizzata da numeri interi:

```
25
8
3
7
10
```

Questo è un array disordinato ma che vogliamo ordinare in maniera crescente (3, 7, 8, 10, 25).
Per raggiungere il nostro scopo possiamo avvalerci di una serie di algoritmi di ordinamento (in inglese ordinamento si definisce "**sort**") di diversa complessità ed efficienza. In generale, maggiore è la complessità dell'algoritmo, e più ardua sarà la sua traduzione in linee di codice (nonché la sua comprensione) e maggiore sarà la sua efficienza.
Iniziamo con il vedere il metodo più semplice di ordinamento.

>> Naive Sort (o sequenziale)

L'algoritmo, come dice il nome stesso, è particolarmente semplice ("naive" in francese vuol dire ingenuo). L'array viene scandito una prima volta dall'inizio alla fine alla ricerca dell'elemento più piccolo (3 nel nostro esempio) e scambiato con l'elemento in prima posizione (25). Per attuare lo scambio senza perdere alcun dato (dovuto alla sovrascrittura), dovremo avvalerci durante la fase di scambio di una variabile di appoggio (variabile ausiliaria).

Viene quindi ri-scandito l'array partendo dalla seconda posizione (visto che la prima è occupata dal minimo assoluto e quindi già ordinata) fino all'ultima posizione, alla ricerca del nuovo mini-

mo. Una volta trovato l'elemento minimo, si ha un nuovo scambio che porta il secondo minimo (7) in seconda posizione.
Si riparte quindi scansionando nuovamente l'array cominciando dalla terza posizione fino all'ultima e attuando lo scambio (se richiesto).
Il processo delle scansioni continua fino a ottenere l'ordinamento dell'intero array.
Svantaggio di tale algoritmo è che **l'intero array viene scansionato più volte anche se per caso fosse già completamente ordinato**.

I vari passi eseguiti con tale algoritmo per ottenere l'array completamente ordinato con il metodo Naive Sort.

>> Bubble Sort

L'algoritmo prende questo simpatico nome dal fatto che i primi elementi che sono ordinati sono posti in fondo all'array e quindi l'ordinamento risale dall'ultimo elemento fino al primo, **come le bolle in un liquido si staccano dal fondo e affiorano in superficie**.
L'array viene scansionato, al massimo, un numero di volte equivalente al numero di elementi che lo compongono.
In ogni scansione si esamina l'array partendo dal primo elemento; se l'elemento esaminato è maggiore di quello che lo segue, i due elementi vengono scambiati (sempre se vogliamo un ordine crescente), altrimenti no. Si passa quindi a esaminare il secondo elemento e come prima si confronta con il successivo (il terzo elemento), ed eventualmente lo si scambia. Il processo continua prendendo in esame tutti gli elementi fino al penultimo e confrontandoli con il successivo. A questo punto la prima scansione è terminata e sicuramente abbiamo depositato sul fondo dell'array (ultima posizione) l'elemento più pesante (maggiore); ma probabilmente anche altri elementi avranno trovato la loro giusta collocazione anche attraverso una sola scansione.
Si riparte quindi con una seconda scansione confrontando sempre il primo elemento e il successivo e così via; il processo di ordinamento è concluso quando non ci sono più scambi da effettuare, e quindi l'array risulta ordinato.
Tale algoritmo ha il vantaggio (nei confronti del metodo precedente) di accorgersi se un array è già ordinato (nessun scambio eseguito) e quindi di **non eseguire una serie di scansioni superflue**.

INIZIO
25 8 3 7 10
1° Scansione
8 3 7 10 25
2° Scansione
3 7 8 10 25
3° Scansione = FINE
3 7 8 10 25
ELEMENTI SOGGETTI A SCAMBI

I vari passi eseguiti dall'algoritmo Bubble Sort per ottenere l'array completamente ordinato.

UN PO' DI MATEMATICA

Il metodo di ricerca binaria è la trasposizione in ambito informatico del metodo di bisezione, usato in analisi numerica per la ricerca delle radici di una equazione.
Ogni volta che applichiamo all'array il metodo di ricerca binaria, stiamo dimezzando lo spazio di ricerca: infatti lo spazio di ricerca dopo "t" tentativi si sarà ridotto di 2t volte.
Conseguentemente, il numero "t" di tentativi necessari per individuare sicuramente la posizione del valore cercato fra "N" elementi è dato dalla formula t = log2 N.
Un ulteriore passo o tentativo serve a leggere il contenuto dell'array nella posizione individuata e a questo punto l'elemento o è stato trovato o non era incluso nell'insieme ordinato.
Praticamente il sistema diventa altamente efficiente se il numero di elementi è estremamente grande. Ad esempio se il numero di elementi è 16, ci basteranno 4 tentativi per trovare l'elemento richiesto (vedi figura); ma se il numero di elementi è 10^{12} (mille miliardi), ci basteranno solo 40 tentativi.
Pensate il notevole risparmio in tempo che si ha rispetto ad un banale metodo di ricerca sequenziale che parte ad esaminare l'array dal primo all'ultimo elemento!

>> Quick Sort

Il Quick Sort è un classico esempio di quella categoria di algoritmi che sfruttano la così detta tecnica "**dividi et impera**" (in inglese, divide and conquer); ossia **separa il problema in tanti sottoproblemi** (più semplici da risolvere), e li risolve per poi riunificarli per ottenere la soluzione complessiva.
All'interno dell'array da ordinare viene selezionato un elemento che prende il nome di "**pivot**" (dal francese perno, cardine), intorno al quale viene attuata la suddivisione in due parti dell'array.
Il sotto-array di sinistra contiene tutti gli elementi dell'array originario, minori del pivot, mentre il sotto-array di destra contiene tutti gli elementi maggiori o uguali al pivot.
La scelta del pivot è estremamente importante nell'efficienza del metodo; tipicamente come pivot si sceglie il primo elemento dell'array o l'ultimo elemento oppure quello centrale; ma esistono anche altri criteri nella scelta del pivot più o meno sofisticati.
In generale attraverso questa suddivisione abbiamo ottenuto 2 sotto-array di dimensione diversa.
Il pivot fa da spartiacque ed è collocato nella giusta posizione, ossia è automaticamente ordinato in quanto sarà maggiore di tutti gli elementi di sinistra (però non ancora ordinati) e minore (o al più uguale) a tutti gli elementi di de-

stra (anch'essi non ancora ordinati). Qualora uno dei due sotto-array risulti essere costituito da un solo elemento, è automatico che si è raggiunto l'ordinamento per quel sotto-array (un solo elemento è auto-ordinato per definizione). Riapplichiamo lo stesso principio (in informatica tale tecnica prende il nome di "ricorsione") a uno dei sotto-array suddividendolo ulteriormente in 2 porzioni: sinistra e destra sempre attraverso la scelta di un nuovo pivot. La suddivisione di un sotto-array continua fino a che non si giunge ad un solo elemento che è automaticamente ordinato. Esaurito l'ordinamento di un sotto-array si passa all'ordinamento di un altro sotto-array. Il procedimento continua fino a che tutti i sotto-array sono stati ridotti ai minimi termini (un solo elemento) e quindi automaticamente tutto l'array risulta ordinato.

Naturalmente, il panorama degli algoritmi di ordinamento è molto complesso e variegato; tra i più importanti citiamo inoltre: l'**Heap Sort** inventato da J.W.J. Williams, lo **Shell Sort** opera di Donald Shell (1959) e il **Merge Sort** ideato niente di meno che da John von Neumann.

INIZIO

25	8	3	7	10

1° Suddivisione PIVOT = 10

8	3	7	10	25

Il pivot è automaticamente ordinato.
Il sotto-array di destra è ordinato perché composto da un solo elemento; quindi:

8	3	7	10	25

2° Suddivisione PIVOT = 7

3	7	8	10	25

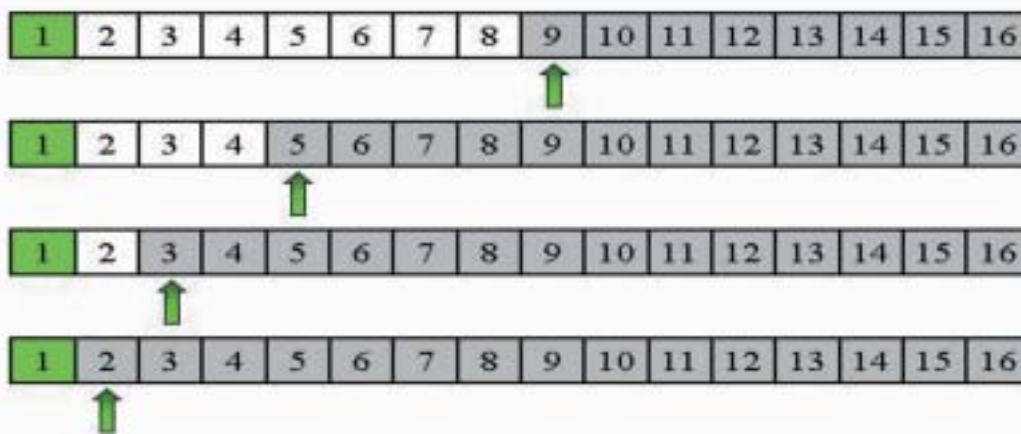
Il pivot è automaticamente ordinato.
Il sotto-array di destra e di sinistra sono ordinati perché composti da un solo elemento; quindi:

FINE

3	7	8	10	25

PIVOT

ELEMENTI ORDINATI

I passi eseguiti dall'algoritmo Quick Sort per ottenere l'array completamente ordinato; come pivot scegliamo in tutti i casi l'ultimo elemento dell'array.

La posizione dell'elemento cercato è stata individuata con 4 tentativi

Elemento da individuare

Elementi scartati

Elemento puntato

La ricerca binaria di un elemento in un array ordinato.

>> Ricerca di un elemento in un array ordinato

Altro problema di interesse pratico è quello della ricerca di un elemento all'interno di un array ordinato; per far questo spesso si ricorre ad un semplice ma efficiente algoritmo che prende il nome di **ricerca binaria.** Se si vuole ricercare un elemento all'interno di un determinato intervallo (ampiezza dell'array), si punta al centro di tale intervallo; implicitamente, individuiamo due sotto-intervalli rispettivamente alla sinistra e alla destra del valore puntato. Siccome l'insieme è ordinato, puntando l'elemento contenuto al centro dell'intervallo può succedere che:

1) **Abbiamo trovato** l'elemento che cercavamo.
2) L'elemento che vogliamo trovare **è minore di quello individuato** e quindi si trova nel sotto-intervallo di sinistra (nel caso l'ordine dell'array sia crescente).
3) L'elemento che vogliamo trovare **è maggiore di quello individuato** e quindi si trova nel sotto-intervallo di destra.

Se l'elemento non è stato individuato, la ricerca continua puntando al centro di uno dei sotto-intervalli (sinistro o destro a seconda delle indicazioni ottenute in precedenza); man mano che il procedimento avanza, verranno trattati sotto-intervalli sempre più piccoli (a ogni passo di ricerca si dimezza l'estensione dell'intervallo) fino a che l'algoritmo di ricerca permetta l'individuazione della posizione dell'elemento cercato.

>> Nel prossimo articolo......

...proseguiremo nel prendere in esame la fase di programmazione costituita dalle istruzioni di selezione, gli operatori condizionali e gli operatori logici.

>>--Robin-->

LINK UTILI

www.cs.brockport.edu/cs/javasort.html
Informazioni dettagliate e animazioni personalizzabili sugli algoritmi di ordinamento.

http://ciips.ee.uwa.edu.au/~morris/Year2/PLDS210/qsort.html
Un'ottima animazione sul funzionamento del Quick Sort.

http://research.microsoft.com/~thoare/
Info sull'autore del Quick Sort [Sir Tony Hoare]

www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Von_Neumann.html
Biografia di John von Neumann

CRYPTO MATRIX

Dall'idea al sorgente, analizziamo una tecnica di cifratura poco sfruttata.

Nella vita quotidiana, dal codice d'accesso del nostro POP Internet, al Bancomat e al PIN del cellulare, **ognuno di noi ha a che fare con una serie di informazioni sensibili** (parole chiave, codici d'accesso) ormai indispensabili, ma che al tempo stesso, in caso di una loro esposizione a occhi poco fidati o peggio, malintenzionati, possono renderci pericolosamente vulnerabili. Se a questi aggiungiamo le recenti possibilità di comunicazione veloce quali posta elettronica o SMS, che per loro natura **lasciano tracce del proprio passaggio in numerose fasi del trasferimento**, va da sé che l'esigenza di criptare i nostri dati personali, da un semplice numero a un testo di molte pagine, sia molto avvertita.

>> Quando proteggere i dati

Non dobbiamo pensare che la tutela delle informazioni sia a esclusivo appannaggio di servizi di sicurezza, apparati dello Stato o industrie. La crescente sensibilità alla riservatezza della nostra sfera personale, giustificata anche dall'esistenza di discutibili impianti di spionaggio come Echelon (una rete di intercettazione utilizzata dai paesi anglosassoni che tiene sotto controllo ogni mezzo di comunicazione), **ha fatto sorgere numerosi sistemi e tecniche di protezione dei dati**. Fra i più noti e affidabili ricordiamo **PGP/GPG, DES** e **Blowfish**. In questo articolo spiegheremo invece l'utilizzo di una tecnica più semplice, basata sul calcolo matriciale, che tuttavia è in grado di offrire un buon grado di sicurezza e invulnerabilità.

>> Cosa sono le matrici

Le matrici, strumento dell'algebra lineare, sono **tabelle di numeri** (in figura 1 potete vederne alcune rappresentazioni), raggruppati in forme stabilite. Il numero di righe e colonne di una matrice può variare; in particolare, quando il numero delle righe è uguale al numero delle colonne, la matrice viene definita "**quadrata**" (più avanti vedremo che noi utilizzeremo proprio una matrice quadrata per i nostri scopi). Una particolare specie di matrice, è la "**matrice identità**", cioè una matrice quadrata composta da elementi nulli con l'eccezione di quelli **posizionati sulla diagonale** che hanno valore unitario (fate riferimento sempre alla figura 1 per un esempio pratico). Fra matrici è possi-

TIPI DI MATRICE

Esempi	Tipo
$\begin{bmatrix}1&3\\2&5\end{bmatrix}$ $\begin{bmatrix}1&2&5\\3&4&7\end{bmatrix}$ $\begin{bmatrix}1&4&5&3&6\\8&7&2&9&3\end{bmatrix}$	Vari ordini
$\begin{bmatrix}1&8&3\\2&3&9\\4&5&7\end{bmatrix}$ $\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$	Matrice e matrice identità
$\begin{bmatrix}1&4\\1&2\end{bmatrix} \times \begin{bmatrix}-1&2\\0.5&-0.5\end{bmatrix} = \begin{bmatrix}1&0\\0&1\end{bmatrix}$	Matrice e sua inversa
$\begin{vmatrix}3&9\\5&7\end{vmatrix} = 3*7-9*5$	Determinante

Figura 1: Varie tipologie di matrici.

Figura 2: Moltiplicando la matrice chiave per la matrice composta dai codici ASCII del messaggio da cifrare, otteniamo un testo criptato.

bile eseguire alcune operazioni algebriche, fra le quali il prodotto. Per eseguire il prodotto di due matrici è necessario che esse siano conformi, cioè il numero di righe della prima matrice deve risultare uguale al numero di colonne della seconda. Per completezza, ricordiamo anche che **il prodotto di matrici non gode della proprietà commutativa**: in altri parole, se invertiamo l'ordine dei fattori, il risultato cambia. Il prodotto di due matrici si realizza moltiplicando le righe della prima matrice con le colonne della seconda.

>> La tecnica di codifica e decodifica

Se noi definiamo una matrice a nostra scelta (in realtà esistono alcune limitazioni, ma le osserveremo più avanti) che potremmo chiamare matrice "chiave" e le affianchiamo una matrice formata dai valori ASCII di un testo, opportunamente resa conforme alla prima (vedi sopra per la definizione), possiamo calcolarne il prodotto. Il risultato sarà ancora una matrice conforme a quella iniziale e che, con opportuni controlli sullo spazio ASCII, **sarà composta da serie incomprensibile di simboli** (caratteri alfanumerici o segni di punteggiatura) corrispondenti ai nuovi valori. Per avere un'idea più precisa, in figura 2 potete seguire dettagliatamente le fasi del processo a cui mi sto riferendo.

A questo punto abbiamo il nostro messaggio cifrato. Ma **in che modo è possibile tornare al testo iniziale in chiaro?** Vediamo prima un esempio semplice e pratico, senza scomodare l'algebra lineare. Immaginiamo adesso di moltiplicare il numero **3** per il numero **9**. Il risultato dell'operazione sarà **27**. Se ora moltiplichiamo **27** per l'inverso del primo fattore (cioè **1/3**) , otteniamo di nuovo il **9** iniziale. A questo punto, la situazione dovrebbe essersi fatta meno caotica. Come starete pensando, se proviamo a **moltiplicare la matrice composta da valori ASCII incomprensibili** (i.e. il prodotto dell'operazione, per capirci il "27" dell'esempio appena visto) **per l'inverso della matrice chiave di partenza**, andiamo a ottenere il secondo fattore della moltiplicazione (il "9" di prima), che altro non è se non **la matrice contenente il testo in chiaro**. Semplice vero?

In realtà, come accennavo all'inizio del paragrafo, dobbiamo tenere conto di alcuni fattori limitanti che riguardano la composizione della matrice chiave. Innanzitutto **è indispensabile utilizzare una matrice quadrata** e in particolare, affinché si possa realizzare il procedimento appena visto, **occorre che la matrice sia invertibile**.

A differenza dell'algebra tradizionale infatti, dove è generalmente possibile calcolare l'inverso di un numero, **non tutte le matrici godono di tale proprietà**. Da ultimo, ma non meno importante, è necessario che **i valori dell'inversa si mantengano interi**. Dicevamo che la matrice deve essere

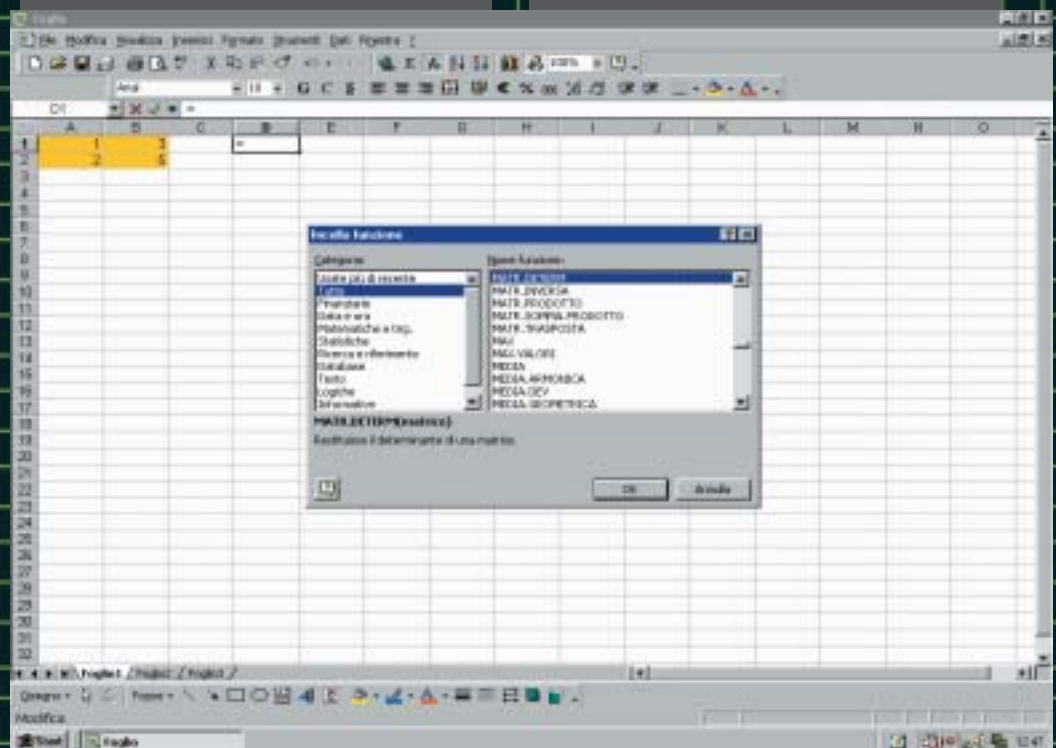



Figura 3: Con un foglio di calcolo è possibile svolgere operazioni sulle matrici, come calcolare il determinante, l'inversa o eseguire il prodotto.

Figura 4: Sorgente del programma Matrix: moltiplicazione delle matrici.

invertibile. Precisamente, perché questo si realizzi, essa deve avere il determinante diverso da zero. Il calcolo del determinante è un'operazione ricorsiva e lunga, specie per matrici composte da molte righe e colonne. Non potendoci soffermare oltre il necessario sull'argomento, vi invitiamo a consultare un testo di matematica per l'osservazione dei teoremi inerenti il calcolo del determinante in casi particolari.
Calcolare l'inversa, invece, è un procedimento piuttosto semplice. Infatti, assegnata una matrice di partenza, la sua matrice inversa moltiplicata per la matrice di partenza produce la matrice identità (vedi sopra per la definizione).

>> Il programma

Come avete potuto osservare nella tabella rappresentata in figura 2, eseguire manualmente i calcoli nei diversi passaggi non è difficile; si tratta piuttosto di operazioni noiose e particolarmente soggette a errori di distrazione. Avvalendoci di un foglio di calcolo (figura 3) potremmo lavorare con facilità sulle matrici e trovarne il determinante, l'inversa o fare il prodotto. In realtà resterebbe da convertire il testo nei rispettivi codici ASCII e in seguito allinearlo alla matrice scelta come chiave, in modo da disporlo in una matrice conforme.

Per rendere le cose più semplici e immediate, **ci viene in aiuto il programma Matrix** che potete scaricare dalla sezione "Contenuti Extra" del nostro sito, sia in forma di **eseguibile per sistemi Win32**, che come **sorgente in C completo e commentato**. Il programma ha un'interfaccia a "console" per rendere facile la conversione su altri sistemi. Non ne siate perciò tratti in inganno: si tratta assolutamente di un programma a 32 bit e non MS-DOS. La versione per Win32 è stata compilata sotto il pacchetto gratuito **Lcc-Win32** e utilizza l'API di Windows unicamente per la gestione della console. Se preferite, potete convertire il programma all'utilizzo della libreria **conio.lib** (in origine sviluppata da Borland per il proprio compilatore) disponibile per diversi pacchetti C. Per portarlo su altri sistemi come **AmigaOS**, **Linux** o **Mac OS**, è richiesta unicamente la riscrittura delle funzioni che gestiscono la stampa a video formattata, facilmente identificabili nel sorgente. Tecnicamente **il programma non fa altro che eseguire i passaggi che abbiamo discusso in precedenza** per quan-

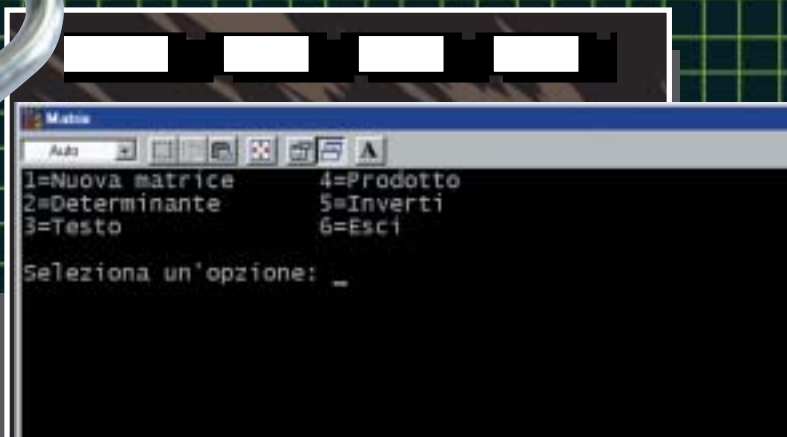



Figura 5: Schermata iniziale del programma

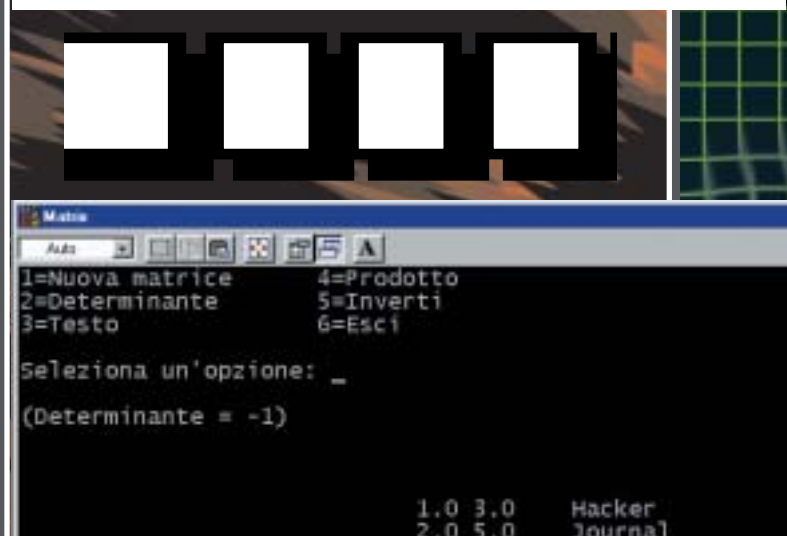



Figura 6: Alla matrice chiave è affiancato il testo da cifrare, opportunamente disposto in una matrice.

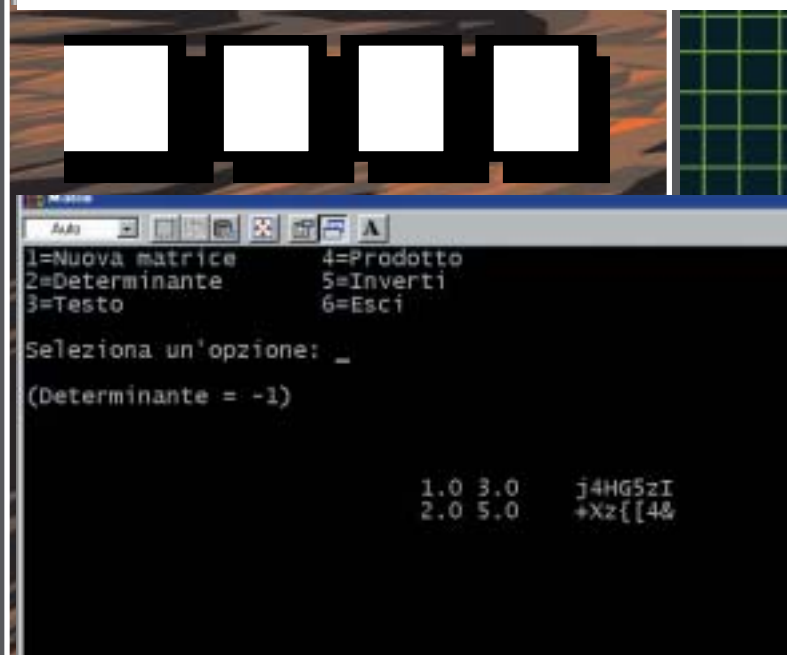



Figura 7: Ecco il testo, dopo aver eseguito il prodotto (opzione 4).

to riguarda le operazioni sulle matrici, oltre che a scomporre il testo da crittografare in una matrice conforme a quella definita come chiave. In figura 4, potete esaminare in dettaglio l'algoritmo che esegue il prodotto di due matrici, come spiegato in precedenza.

>> Utilizzo del programma

Per cominciare, è necessario **inserire una matrice chiave**. Per fare questo, scegliete l'opzione "**1**" e digitate in seguito **2**, per utilizzare una matrice di secondo ordine. Il programma vi chiederà adesso di digitare i valori che compongono la matrice. Inserite, come nell'esempio in figura 6, i valori **1**, **2**, **3** e **5**. Al termine di questa fase, potete modificare la matrice appena inserita oppure, rispondendo con "**n**" alla domanda, tornare al menu principale. A questo punto dobbiamo accertare che le due condizioni fondamentali che dicevamo in precedenza siano rispettate. Con le opzioni "**2**" e "**5**" , controlliamo rispettivamente che il determinante sia diverso da zero e che i valori della matrice inversa siano ancora numeri interi. Se abbiamo invertito la matrice, possiamo tornare a quella di partenza premendo nuovamente "**5**". Bene, superato questo passaggio, non ci resta che **impostare il testo da codificare**. Scegliete "**3**" e scrivete una frase a vostro piacimento. Il testo verrà scomposto automaticamente dal programma in una matrice conforme a quella chiave. Per cifrare la frase, eseguite il prodotto selezionando l'opzione "**4**". Ecco, l'insieme dei caratteri apparentemente senza senso, rappresenta adesso il testo codificato (figura 7). Per tornare al messaggio in chiaro, è sufficiente invertire la matrice chiave (opzione "**5**") e ottenere nuovamente il prodotto (tasto "**4**"). Il messaggio apparirà di nuovo in una forma comprensibile. Ricordiamo anche che le due matrici possono essere moltiplicate un numero infinito di volte. Successivamente, per tornare al testo leggibile, dobbiamo solo ricordarci di moltiplicare l'inversa per il testo criptato lo stesso numero di volte eseguito in precedenza. Questo particolare aggiunge un ulteriore livello di difficoltà, poiché il numero dei prodotti è variabile e deciso dall'utente. Poiché le due matrici devono essere disposte in maniera conforme, può capitare che un testo non entri per intero nella matrice: in tal caso è utile **aggiungere uno spazio finale** o adattare la matrice chiave, cambiandone per esempio l'ordine.

Bene, a questo punto non mi resta che concludere, lasciandovi con un saluto, naturalmente in codice: `$1$:!w/|3VNb'sG<Y?gC` (matrice chiave: 2 3 3 5) .

Fabio Benedetti

AFFIDABILITÀ E APPLICABILITÀ

La tecnica crittografica analizzata in queste pagine, appartiene alla famiglia dei codici "a sostituzione". Con questa terminologia si indicano quei sistemi crittografici dove a un componente da codificare ne viene sostituito un altro. Naturalmente a differenza di tecniche più semplici, come il cosiddetto cifrario di Cesare, dove a ogni valore ne corrisponde sempre e univocamente un altro (per esempio alla lettera "i" si sostituisce la "e", alla "v", la "a" e così via), nel nostro caso la lettera "f" potrebbe prima essere cambiata in una "a", ma subito dopo mutarsi in una "b". Inoltre, il numero di combinazioni delle matrici chiave offre un certo margine di inattaccabilità (soprattutto se si ricorre a matrici di ordine superiore al secondo), anche ipotizzando il ricorso a tecniche "a forza bruta" per l'individuazione della chiave. In realtà, ciò che paradossalmente rende il sistema sufficientemente sicuro, è la scarsa diffusione. Affinché un testo criptato possa essere svelato, infatti, è necessario conoscerne il metodo impiegato durante la codifica. Disassemblare un programma e studiare un algoritmo dal sorgente in assembly non è un'operazione così immediata e di facile realizzabilità. Questo tipo di crittografia inoltre, grazie anche alla relativa velocità di decodifica, è particolarmente adatta ai testi. Pensate alle frasi contenute all'interno di un eseguibile, che riportano per esempio il nome dell'autore o altri dati personali.
Tipicamente, queste informazioni sono facilmente modificabili attraverso un semplicissimo editor di file. Oppure potremmo utilizzare questa tecnica per nascondere messaggi all'interno di altri file che non verrebbero così osservati indistintamente da tutti. Lo stesso programma Matrix si presta a ulteriori sviluppi, come il salvataggio e la lettura dei messaggi. Un'altra possibilità sarebbe infine quella di memorizzare, insieme al messaggio, la chiave di codifica di volta in volta utilizzata. Insomma, come sempre esistono pochi limiti al miglioramento, se non l'applicazione, la voglia di fare e la capacità.
Ultimo, indispensabile commento: il metodo e il programma che presentiamo qui sono a scopo di studio ed esercizio: per proteggere i propri dati nel modo più sicuro, raccomandiamo di utilizzare programmi e algoritmi ritenuti sicuri e affidabili, come quelli citati all'inizio dell'articolo.